

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property
Organization
International Bureau(43) International Publication Date
1 April 2004 (01.04.2004)

PCT

(10) International Publication Number
WO 2004/028077 A1

(51) International Patent Classification: H04L 9/32

(21) International Application Number:
PCT/EP2003/007829

(22) International Filing Date: 18 July 2003 (18.07.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
02020583.7 17 September 2002 (17.09.2002) EP

(71) Applicant and

(72) Inventor: PITSOS, Errikos [DE/DE]; Florian-Geyer-Str.
10, 81377 München (DE).(74) Agent: GRÜNECKER, KINKELDEY, STOCKMAIR
& SCHWANHÄUSSER; Maximilianstrasse 58, 80538
München (DE).(81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.(84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

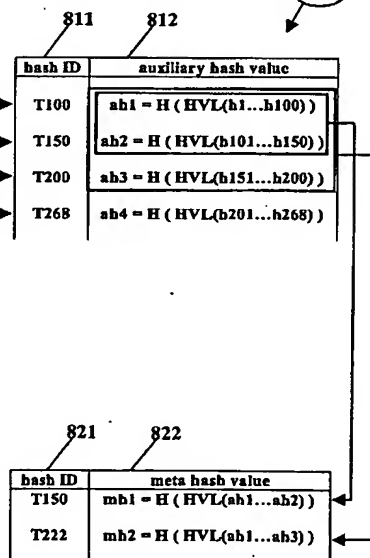
Published:

— with international search report

[Continued on next page]

(54) Title: METHODS AND SYSTEMS FOR PROVIDING A SECURE DATA DISTRIBUTION VIA PUBLIC NETWORKS

time	data ID	data	hash value
T1	1	D1	$h1 = H(D1)$
T2	2	D2	$h2 = H(D2)$
⋮	⋮	⋮	⋮
T100	100	D100	$h100 = H(D100)$
T101	101	D101	$h101 = H(D101)$
T102	102	D102	$h102 = H(D102)$
⋮	⋮	⋮	⋮
T150	150	D150	$h150 = H(D150)$
T151	151	D151	$h151 = H(D151)$
⋮	⋮	⋮	⋮
T200	200	D200	$h200 = H(D200)$
T201	201	D201	$h201 = H(D201)$
⋮	⋮	⋮	⋮
T222	222	D222	$h222 = H(D222)$
T223	223	D223	$h223 = H(D223)$
⋮	⋮	⋮	⋮
T268	268	D268	$h268 = H(D268)$
T269	269	D269	$h269 = H(D269)$



(57) Abstract: A server in a public key system stores a list of fingerprints of digital data. Another fingerprint is computed for this list of fingerprints and provided to a client terminal. A client terminal in a public key system obtains a list of fingerprints of digital data from a first source in this system. The client terminal further obtains a fingerprint for that list of fingerprints from a first source as well as from a second source for comparing both obtained fingerprints.

WO 2004/028077 A1

BEST AVAILABLE COPY